JOURNEYS TO TREASURY

Striving for the summits of treasury with **BNP PARIBAS - EACT - PwC - SAP**

DATA ANALYTICS: HOW TO GIVE MEANING TO YOUR BIG DATA?

REGULATION, COMPLIANCE AND GEOPOLITICS: HOW TO STAY AHEAD OF THE GAME?

CYBERSECURITY: HOW TO MANAGE AUGMENTED RISK IN A DIGITAL WORLD?

BNP PARIBAS
The bank for a changing world

EACT THE EUROPEAN ASSOCIATION OF CORPORATE TREASURERS

pwc

SAP®

THERE ARE MANY JOURNEYS TO TREASURY

DESIGN YOUR OWN:
WWW.JOURNEYSTOTREASURY.COM

BNP PARIBAS
The bank for a changing world

THE EUROPEAN ASSOCIATION OF CORPORATE TREASURERS

pwc

SAP

Content

FOUR TRENDS WITH GAME-CHANGING POTENTIAL 6

DATA ANALYTICS: HOW TO GIVE MEANING TO YOUR BIG DATA? 8

REGULATION, COMPLIANCE AND GEOPOLITICS: HOW TO STAY AHEAD OF THE GAME? 15

CYBERSECURITY: MANAGING AUGMENTED RISK IN A DIGITAL WORLD 22

CLOSING THOUGHTS 29

A JOURNEY TO TREASURY ROADMAP

PHILOSOPHY OF THE REPORT

FINDING A CLEAR PATH FORWARD

Some changes seem to be running at the speed of light. In this morass of hard trends and cosmetic swirls, how do we distinguish the trend from the trendy? How do we know which changes are truly disruptive, and which are merely potentially transformative? Which technologies are going to have the biggest impact on decision making? And, of the many initiatives put forward, which will be pivotal to the corporate treasurer's journey?

Journeys to Treasury is an initiative, a reflection, aiming to accompany finance professionals through the intricate labyrinth of treasury, avoiding dead-ends and finding a clear path forward. The approach is simple: a conversation between BNP Paribas, the European Association of Corporate Treasurers (EACT), PwC and SAP. In essence, between the financial services industry, the association of professionals, the consultant and the systems provider. The discourse is distinctive – concepts may go out of fashion, but talk never will. Now in its second year, *Journeys to Treasury* is the product of a long-standing relationship between the four top financial industry players.

The report is unique in the world of corporate treasury – a collaborative, multi-faceted view, squarely aimed at the professional in a volatile landscape. Businesses change, and the regulatory and technological context in which we do business changes; how innovation happens and how IT systems are designed are changing too. Each of the four *Journeys to Treasury* partners offers their own expertise, distilled from their own journey.

Not simply about hot topics, the report goes for a focused, intelligence-led, collective and inclusive analysis of critical themes which are set to redefine treasury, offering a clear-sighted and sure-footed way forward for corporate treasurers setting out on their own *Journeys to Treasury* in this ever-changing world. Bon voyage!

Executive summary

From a survey of more than 100 treasurers who attended the 1st 2017 EACT Summit, followed by a panel discussion and one-to-one interviews, three issues emerged for discussion in this second edition.

Regulation and cyber threats were the top two items on their agenda going forward. However, Big Data that ranked lower on the list, probably resulting from a misunderstanding given the opportunities that data can bring when properly exploited. We tested how resonant these topics are within the European corporate treasury community by asking participants at the EACT Summit: "Which of the following factors will impact your treasury strategy in the coming years"?

The result is *Journeys to Treasury 2017*, a report structured around three key sections and including several case studies, serving to make ideas and concepts more tangible. As an introduction, the report also provides an update on other topics such as Blockchain, Instant Payments and Fintechs.

Data analytics: give meaning to your Big Data

Not yet fully on corporate treasury radar, Big Data refers to the large volume of data inundating businesses every day. But it is not the amount of data that is important: It is what organisations do with it that matters.

Big Data, often associated with artificial intelligence (AI) and machine learning, can be analysed for insights that lead to better decisions and effective business strategies. The tools already exist. What is probably next on the agenda is a change of mindset so that corporates capitalise on the value that data can bring. Then, they need to identify the issues data analytics can help to solve - FX and daily investment decisions are in the frame, ripe for exploration. To illustrate this, *JTT 2017* shows how a global leader in the flavours industry turned to robotics and AI to provide the treasurer with a consolidated FX exposure in just 30 minutes.

Regulation, compliance and geopolitics: stay ahead of the game

Treasurers continue to be hit by an avalanche of direct and indirect regulations. It is a case of comply or risk sanctions, fines, and reputational damage. Looking beyond treasury to keep up with developments is crucial, and precious advice can be found in colleagues at all levels. The risk brought by non-compliance with the EU's General Data Protection Regulation (GDPR) makes working closely with data protection colleagues a must. The section's case study shows what treasurers have to gain by working hand-in-hand with tax experts, and by putting a strong focus on substance and transparency.

Cybersecurity: managing risk in a digital world

Fraud prevention is a company-wide responsibility. With individual staff often the weakest link, training is paramount. Surveys show that staff who undergo awareness training are glad they did, and that being aware of the risks makes them better equipped to deal with them. Regular staged simulations of cyber-attacks are an essential wakeup call to highlight the dangers an organisation faces. Over-sharing on social media platforms can also help fraudsters get access to vital company assets. After experiencing such a fraud, a leading agro-industrial group both adapted its internal culture and updated agreements with its financial partner.

Thank you

for joining us on our journey.

FOUR **TRENDS** WITH GAME-CHANGING POTENTIAL

Blockchain, robotics, instant payments and Fintechs were among the hot topics of the first edition of *Journeys to Treasury* in 2016. Although they might not be right at the top of the treasurer's list this year, the issues remain potentially transformative. Here's a quick update on their current status.

According to physicist Stephen Hawking, "the rise of **artificial intelligence** is likely to extend job destruction deep into the middle classes". Do treasurers have anything to fear from the rise of robots? Automation is already being used for time-consuming and error-sensitive tasks, and treasury departments have been getting leaner while treasurers progressively took on a more strategic role. The next step in automation is **machine learning** that can facilitate reconciliation and help build data to feed predictive analysis. This, in turn, can help prevent cyberattack and fraud. That makes Artificial intelligence (AI) more about extending treasury's scope than further squeezing human resources.

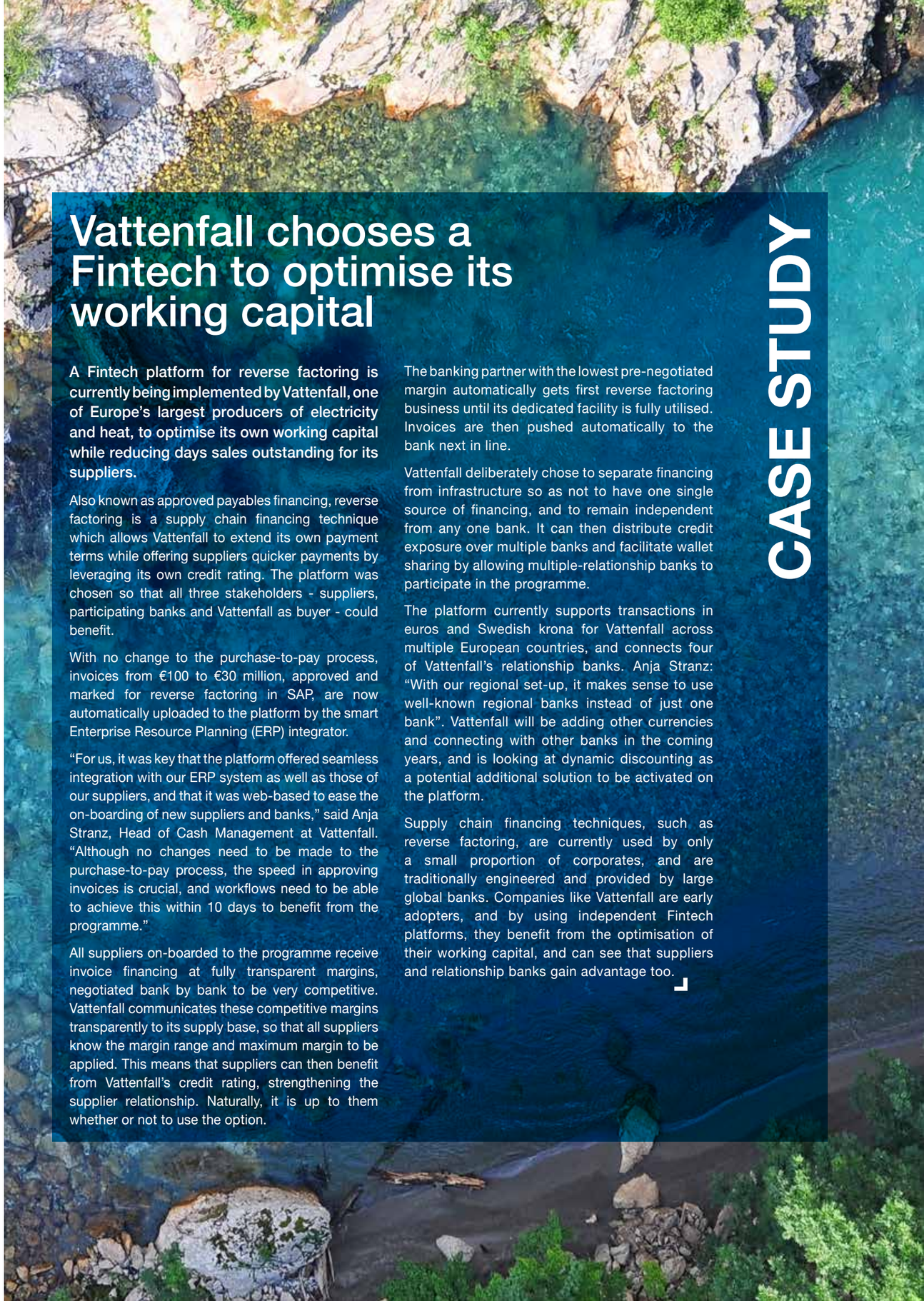
However, treasurers must first have the necessary machines, and automate payment processes as much as they can. Only then can machine learning come into play and convert data into the virtuous circle: the more we know, the more we learn. Imagine a world where useful information is proactively provided to corporate treasurers, with no need for them to ask.

Fintechs can generate genuine value and globally accelerate innovation, and yet with so many in existence, how can we tell which solutions really work? What we must do is identify which innovations could bring real value to our treasury management chain and fit smoothly into existing structures from the regulatory, compliance and technical standpoints.

For real-time clearing, settlement, reporting and visibility, blockchain technology is promising, and its founding principles may make it a game changer but, for now at least, use cases are patchy and the benefits are as yet unclear. The distributed ledger remains a trend to be closely monitored but is indisputably a basis for tangible innovation.

Instant payments have gone live in many countries across the world, but the trend is recent and few nations can boast significant success as yet, although a number are worthy of attention. Denmark is a frontrunner with the implementation of a very successful scheme. In Spain, Bizum is a mobile interbank application allowing payments to be made and received with immediate confirmation. In Australia, the banking community has scheduled the implementation of instant payments by the end of 2017. And in the US, several initiatives are underway, among them a business-to-business platform, a Federal Reserve System taskforce to support implementation of instant payment solutions, and Zelle, a P2P mobile payment initiative supported by about 30 banks so far.

Across Europe, for instant payments to become an alternative means of payment, a new infrastructure must be built, requiring significant investment. The journey has begun, but it will take time, effort and commitment from all the stakeholders for a pan-European instant payment market to emerge. Meanwhile, instant payments are likely to flourish at local level in several countries – a trend that we must definitely keep a close eye on.



CASE STUDY

Vattenfall chooses a Fintech to optimise its working capital

A Fintech platform for reverse factoring is currently being implemented by Vattenfall, one of Europe's largest producers of electricity and heat, to optimise its own working capital while reducing days sales outstanding for its suppliers.

Also known as approved payables financing, reverse factoring is a supply chain financing technique which allows Vattenfall to extend its own payment terms while offering suppliers quicker payments by leveraging its own credit rating. The platform was chosen so that all three stakeholders - suppliers, participating banks and Vattenfall as buyer - could benefit.

With no change to the purchase-to-pay process, invoices from €100 to €30 million, approved and marked for reverse factoring in SAP, are now automatically uploaded to the platform by the smart Enterprise Resource Planning (ERP) integrator.

"For us, it was key that the platform offered seamless integration with our ERP system as well as those of our suppliers, and that it was web-based to ease the on-boarding of new suppliers and banks," said Anja Stranz, Head of Cash Management at Vattenfall. "Although no changes need to be made to the purchase-to-pay process, the speed in approving invoices is crucial, and workflows need to be able to achieve this within 10 days to benefit from the programme."

All suppliers on-boarded to the programme receive invoice financing at fully transparent margins, negotiated bank by bank to be very competitive. Vattenfall communicates these competitive margins transparently to its supply base, so that all suppliers know the margin range and maximum margin to be applied. This means that suppliers can then benefit from Vattenfall's credit rating, strengthening the supplier relationship. Naturally, it is up to them whether or not to use the option.

The banking partner with the lowest pre-negotiated margin automatically gets first reverse factoring business until its dedicated facility is fully utilised. Invoices are then pushed automatically to the bank next in line.

Vattenfall deliberately chose to separate financing from infrastructure so as not to have one single source of financing, and to remain independent from any one bank. It can then distribute credit exposure over multiple banks and facilitate wallet sharing by allowing multiple-relationship banks to participate in the programme.

The platform currently supports transactions in euros and Swedish krona for Vattenfall across multiple European countries, and connects four of Vattenfall's relationship banks. Anja Stranz: "With our regional set-up, it makes sense to use well-known regional banks instead of just one bank". Vattenfall will be adding other currencies and connecting with other banks in the coming years, and is looking at dynamic discounting as a potential additional solution to be activated on the platform.

Supply chain financing techniques, such as reverse factoring, are currently used by only a small proportion of corporates, and are traditionally engineered and provided by large global banks. Companies like Vattenfall are early adopters, and by using independent Fintech platforms, they benefit from the optimisation of their working capital, and can see that suppliers and relationship banks gain advantage too.

GIVE MEANING TO YOUR BIG DATA

DATA ANALYTICS

Big Data can be an unstructured inundation of ones and zeros flooding into companies and organisations. But could this be one of those subjects where we don't need to understand how something works to be able to exploit it to the full?

Add a generous dose of data analytics and your Big Data is magically transformed into evidence, allowing organisations and companies to make better financial and business decisions. The future is already here, and does not require a PhD in advanced anything. Just an ability to focus on real-world practical solutions.

Not just internet data moguls

In the 2016 report, we talked of Big Data as being the ability to handle the three Vs (volume, velocity and variability) of incoming data, and harness them for the treasurer's needs. However, the systems and skillsets required were beyond what most treasuries could extend to, with the exception of those serving internet retailers or global search engines. Even in these types of companies, treasury was often merely the customer of Big Data, not the producer.

Should Big Data really be a focus for treasurers? Most treasury data is not unstructured terabytes, as talked about by data scientists. Rather it is relatively centralised and organised, comprising cash balances, bank statements and financial transactions.

The treasurer's main focus should therefore be on how to display existing data in a sufficiently meaningful way to quickly inform complex decisions, rather than on how to manage data lakes. The

Big Data: should it really be a focus for treasurers?

focus for many treasurers this year is the reality of implementing something quick and impactful using data analytics rather than theorising on the future possibilities of Big Data.

What is data analytics? Wikipedia says that data analytics is "the process of inspecting, cleaning, transforming and modelling data with the goal of discovering useful information, suggesting conclusions and supporting decision making". This is exactly what treasurers need, but many are put off by the thought that it will require expensive machine learning, artificial intelligence or powerful processing platforms they can neither afford nor have the capacity to implement for treasury alone.

The good news is that not only the thinking, but also the tools have evolved greatly in the last few years.

Today, **machine learning tools are available for download** for as little as €20,000, and sometimes for free. If you are operating the latest version of your ERP system, you may already have in-memory computing. If neither of these options is open to you, there is still the possibility of outsourcing your data analytics and artificial intelligence to a Fintech provider who can shield treasury from the complexity of the task and deliver the end result analysis direct to the user.

It is a change in mind-set not tool-set which is the real challenge. If the tools are available relatively cheaply on the internet, what is really holding us back? Is it the fear that "this is complex stuff"? For €180, a five-week course on data analytics through Coursera is available which will give any treasurer a great start and at least put them in a more informed position when discussing the topic with 'experts'.

How can treasurers use data analytics?

Identify the business issue: This is often the most difficult step since treasurers need to be as precise as possible to identify the data and processing capabilities they need. Even in the simplest of examples, such as cash flow forecast, there may be many stakeholders (for example, short-term liquidity manager vs. long-term debt manager) who each have a slightly different perspective on:

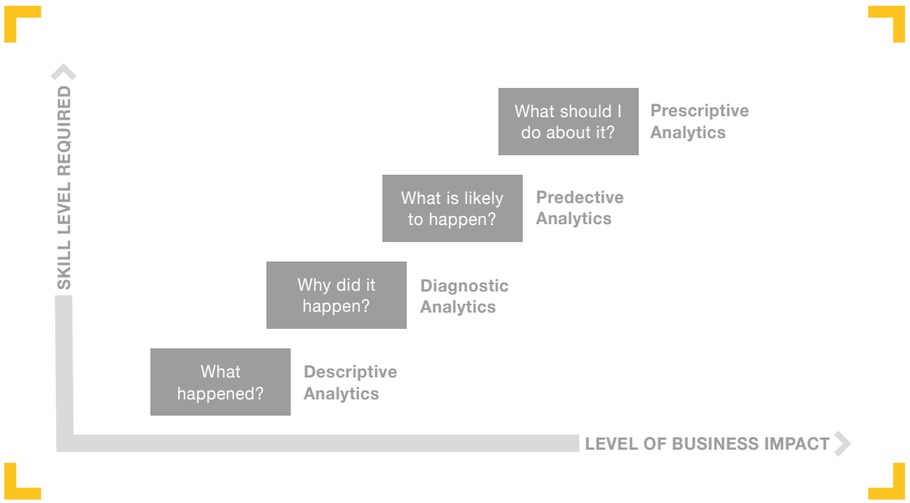
- the time horizon,
- the time buckets,
- the frequency required for refreshes,
- the level of detail in line items and sub-line items required to explain variances,
- the different display levels needed, and hierarchical keys that must be embedded in the data set,
- the sufficient level of accuracy.

Data Sources: While there will be an ideal data set to meet requirements, it is unlikely within most complex multinationals that this resides in one handy data warehouse. Multiple sources will have to be used and proxies created when core data is not readily available in a digestible format.

Data Exploration: Gather it, clean it and enrich it. Together with the prior two steps, this is often the most labour intensive part of the project. However, once the methodology has been designed, it is possible to implement algorithms to automate the process (necessary when forecasting at a high frequency).

Data analytics: The tools only really come into play at this stage. You must identify the most appropriate form of data analytics to solve your issues and achieve the required impact, for example:

THE BIG DATA ANALYTICS CONTINUUM



For a true cash flow forecast, treasurers want to be able to predict the future with some degree of accuracy.

- If you only want to see *what* happened, e.g. a cash position, not much sophistication is needed, and it is more about presentation;
- If you'd like to understand *why* something happened, more sophisticated correlation analysis is required;
- For a true cash flow forecast, you want to be able to predict the future with some degree of accuracy. This is where machine learning tools that constantly update the above correlation rules with newly observable trends are useful to continually enhance their prediction of *what is likely* to happen. Many treasuries are now at this stage, using simple consolidation of bottom-up templates from each controller, but in parallel using their own algorithms to either make cleansed data more readily available or get real-time data, and extrapolating to give a more accurate result;
- If your cash balance is x, the model predicts y more will come in, and your revolve costs are z%, how much should you invest, in which fund, and for how long? This is where some treasurers have now started using AI in the form of robotics.
- **Data visualisation - a picture tells a thousand words**: Where robotics are not available and large quantities of data need to be digested by humans, data analytics/presentation tools (like *Tableau* and *QlikView*) can easily be leveraged and plug well into most Treasury Management Systems (TMS) databases for quick and stunning results. Many TMS providers, after years of developing their own reporting platforms, have come to the conclusion that offering open Application Programme Interfaces (APIs) to these tools is the best option for their clients.

The power of robotics

As in the example above, the use of data analytics has the power not only to make the treasurer's life more informed, but also less repetitive. By utilising AI based on data analytics, treasurers are starting to develop robotics to assist with, for example:

- **Automated FX hedging (algorithmic trading for the masses)** – What used to be the preserve of algorithmic traders is now employed, in one form or another, by some treasurers who use the above tools to not only more accurately forecast their FX exposures, but then hedge, book and account for these according to specific policies, all automatically. This allows for archived micro-level hedging and matching, without significant human effort.
- **Automated daily liquidity investments** – In a more simplified way, the same techniques can be used to invest short-term surplus liquidity in approved instruments and tenures. This is already offered by some banks even where the internal capabilities do not exist.

By using data analytics and AI in this way, treasurers are not only removing the repetitive drudgery from daily treasury activities, but allowing more real-time policy monitoring, even outside of office hours, with the added capability of automating reactions to events.

Some surveys predict that up to a third of today's jobs will no longer exist ten years from now due to robotics, meaning that treasurers need to start preparing themselves and their departments for this phenomenon. Which parts of the back, front and middle offices can be automated using data analytics and artificial intelligence?

With Big Data come big responsibilities – Although the above data analytics tools are freeing the treasurer up to be much more proactive rather than reactive, there are other considerations to bear in mind during the design and maintenance of a treasurer's data analytics framework.

One of the growing concerns, and one which is still evolving, is data privacy. Treasurers must be aware of what data they keep, and how and where they keep it. Regulation is increasing rapidly, especially on personally identifiable information (PII). The European GDPR (see page 18), and each of its regional equivalents, could impact the data kept in a payment factory for example – including names of authorised signatories, passports and other KYC (Know Your Customer) documents.

Data set design, cleansing, storage and security must be built into overall data analytics strategies.

KEY POINTS TO REMEMBER

- **The question is not when and how you plan to use data analytics, but rather what is stopping you from doing it already?**
- **The most difficult part, and therefore where most time should be spent, is defining the problem statement and the desired outcome.**
- **Consult carefully with experts, not only on how to build the output but on how to manage the collected data within the regulations**
- **Thanks to robotics and AI, the treasury department of a global leader in the flavours industry can have a consolidated FX exposure in just 30 minutes.**

CASE STUDY

Givaudan's treasury turns to robotics

Givaudan is a CHF 5bn revenue company and the global leader in the flavour industry. As such, the company has complex FX exposures, intercompany transactions and cash flow patterns to track, analyse and manage.

The Past

With a limited treasury team of seven (including back and middle office operations) the question is how to best deploy scarce resources. That is why Givaudan's Head of Market Risk, Antonio Nota, turned to Robotic Process Automation (RPA).

Givaudan uses SAP Treasury as their main TMS, and captures their FX deals and counterparty risk within the system. However, despite having a relatively straightforward FX hedging policy, staff were faced with 3.5-4 hours per day of manual, repetitive effort to manage FX exposure, including:

- Capturing the exposures of more than 23 entities in the TMS;
- Pricing and execution of 50-60 intercompany hedges to transfer the exposure to HQ treasury and subsequently input into the system;
- Identifying netting opportunities and deriving the final exposure per currency for the group;
- Hedging treasury's position externally, within their counterparty credit policy.

As a matter of fact, like many FX hedging programmes, it meets the classic criteria for RPA.

The process is:

- highly manual,
- high frequency,
- repeatable,
- rules- or policy-based.

The Present

As a first step, Givaudan used its systems provider's standard functionality to capture their underlying G/L exposure as an automated process directly from the business entities.

Using a smart add-on, they automated the rest of the process. Put simply, they have taught the TMS their treasury policies and thresholds. The system has been enhanced to contain the parameters of Givaudan's FX policies and hedge percentages, per currency and per entity. After setting these boundaries in the system, the team developed a series of automated functions where the system automatically identifies and executes the appropriate hedge with each internal counterparty, at the day rate uploaded from Reuters, in order to have an arm's length trade vis-à-vis the tax authorities of the countries of the companies involved. Since Givaudan was performing exposure management for more than 23 entities and using up to 50-60 trades per day, this has saved significant effort and CHF 15 million.

The final product of the RPA is the consolidated net Group FX exposure, delivered to the treasurer in just 30 minutes. The information is provided early, allowing the treasurer more time to determine the best timing and conditions to trade their exposure in the market.

The Future

For now the company still performs the final deal with their banks manually, as they assess the robustness of the input data (to avoid the garbage in – garbage out problem). However, in the future they may, like some advanced corporates, automate this final execution of the deal with their external counterparties, which for many is also a highly manual, repetitive, rules-based process.

CASE STUDY

Advice from the wise

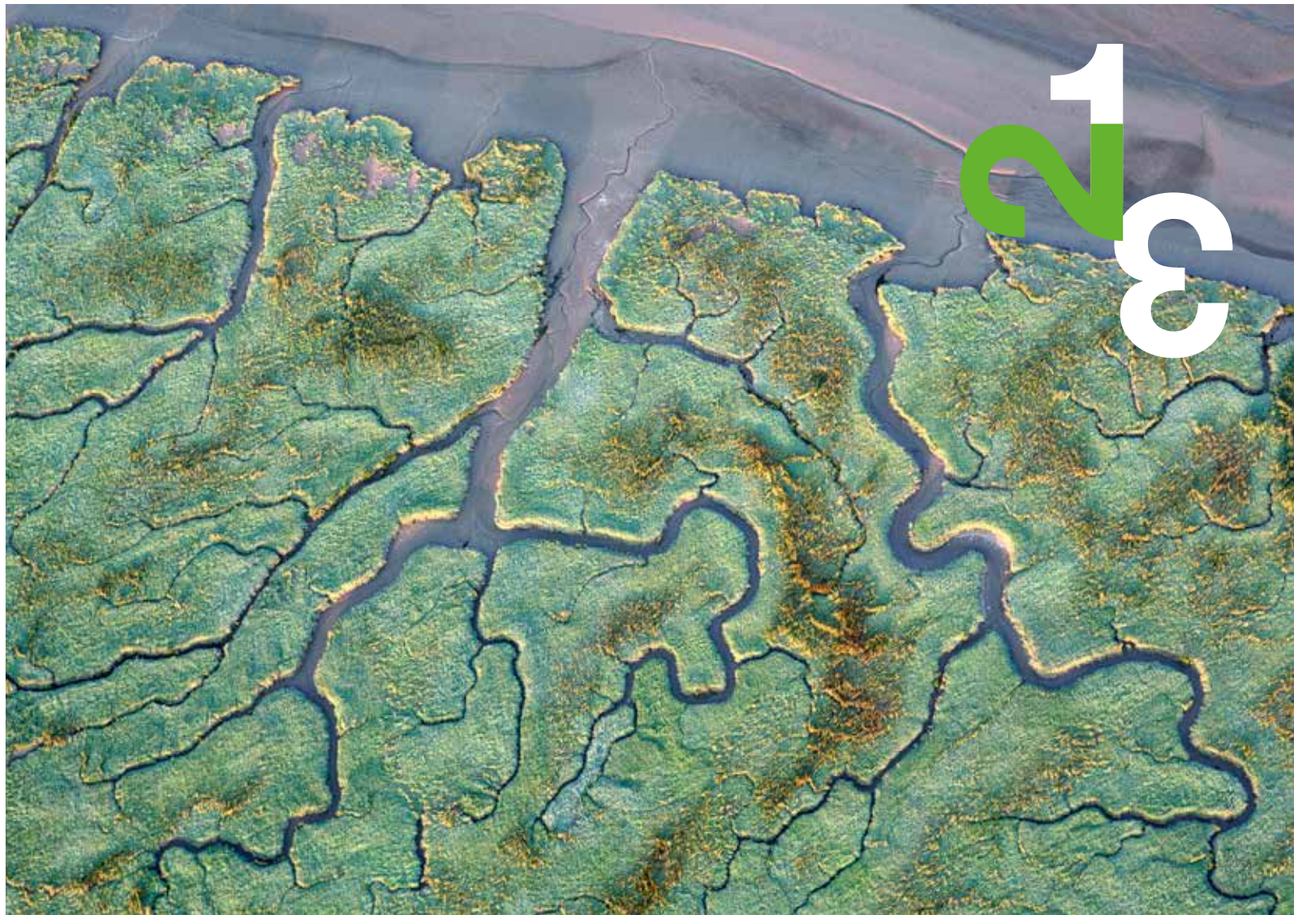
Antonio Nota, Group Treasurer at Givaudan, has sage advice for anyone embarking on such a project: map it out, simplify the process as much as possible, and try the process manually. This has the twin benefits of allowing you to refine the process before capturing it in the system, and identify a back-up solution easily replicable by humans should systems problems arise.

His advice is to constantly challenge yourself and look for other associated processes to pull into the RPA. For example, even after executing his hedges, Nota goes further and applies automated alerts to be notified of any material adverse change in his counterparty's credit ratings (as measured by traded CDS spreads). These alerts are courtesy of another SAP add-on which combines the outstanding deal valuations with the cash held at the same banking group and compares these against CDS spread thresholds in their counterparty risk polices.

The use of RPA is perhaps an ongoing continuum of automation, but with advances in technology it is now moving at a rate, and with a scope, that is often only limited by our imagination and enthusiasm.

HOW TO STAY AHEAD OF THE GAME

REGULATION, COMPLIANCE AND GEOPOLITICS



The constant churn of financial regulation has caused much debate among corporates. Added to this are the shockwaves of the UK's departure from the European Union, the arrival of a new administration in the US and other major shifts in the political and social landscape, in Europe and further afield. What can CFOs and treasurers do to stay ahead of the game in this challenging and fast-moving scenario?

Treasurers' agendas continue to be dominated by a wide range of changes in regulation, compliance requirements and accounting. Corporate treasurers have already had to invest heavily to update policies, processes and systems to comply with SEPA, Dodd-Frank and the European Market Infrastructure Regulation (EMIR), and deal with the administrative burdens triggered by Know Your Customer (KYC) and Foreign Bank Account Reporting (FBAR). Add to this assessing the impact of changes in fiscal legislation and accounting policies such as IFRS 9 and, more recently, funding and investment strategies in the wake of new capital and liquidity rules from money market fund reform, and you get the picture.

In addition to this compliance burden, geopolitical and governmental change add further layers of uncertainty and complexity. As a result, many treasurers find it a challenge to balance their budgets, given the effort required for compliance, while at the same time making treasury more effective and resilient.

Potential damage down the line

In the aftermath of the most recent financial crisis, many corporate treasurers have made significant progress in dealing with the practical implications and operational impacts of regulatory initiatives. However, the more recent developments have lifted the regulatory discussion to a higher level, attracting the attention of executive management and boards. But significant potential financial consequences - penalties - and reputational damage, are generating opportunities as well as risks.

It would be hard to find a corporate treasurer who has not yet been asked questions about the broader business implications resulting from Brexit and the company's GBP exposures, or about potential changes in tax and regulation policies under the new US administration. These are strategic questions and corporate treasurers can (and should) play a proactive role in finding the answers, providing a prime opportunity to continue to raise their profiles and drive real business value.

Geopolitical changes

Over the past year, there have been several unexpected political changes across the globe. Major events included the UK vote to leave the European Union, the arrival of the new US administration and recent elections in Europe.

These political events and potentially drastic changes to policies and international trade models create a climate of uncertainty and nurture market volatility. The slightest unpredictable event shakes up markets and entire economies. The main challenge for companies and their treasury departments is to filter out the noise and avoid overreaction.

While the consequences of Brexit remain unclear, the key economic objectives of the newly elected administration in the US have been widely covered in the media: tax reform, infrastructure investment and less regulation.

Deregulation has been put in motion with the US administration having recently dramatically scaled back the Dodd-Frank Act. The European Commission, for its part, submitted a proposal to simplify and reduce the impact and compliance burden of EMIR for non-financial counterparties.

Compared to the US, the deregulation in the EU is expected to be limited, and is likely to fit within the pre-defined agenda of the Regulatory Fitness and Performance Programme (REFIT), aiming at financial stability and growth.

Flexibility and resilience

Corporate treasurers must constantly navigate these geopolitical risks and strive to create a flexible and risk-resilient treasury organisation, knowing that it is virtually impossible to build a pre-defined strategy.

One way to achieve this is to use scenario or sensitivity analysis on, for example, the FX exposures leading up to a major event such as Brexit. The direct impact of the process on key company metrics, such as FX gains and losses, can also be mapped or, going even further, so too can the secondary impacts on business factors such as economic competitiveness and pricing flexibility.

The main challenge for companies and their treasury departments is to filter out the noise and avoid overreaction.

Building such scenarios requires a profound and holistic understanding of not only the risk, but also the processes and business areas that could be affected. This requires that treasurers consult and engage with internal and external stakeholders to bring diverse perspectives together.

Increasing transparency

Treasury operations will also be influenced by increasing transparency towards tax authorities. One of the BEPS (Base Erosion and Profit Shifting) action points specifically focuses on the documentation requirements for multinationals.

From financial year 2016 onwards, many groups have needed to prepare a transfer pricing master file to provide the tax authorities with a clear picture of a group's overall activity, their business strategy, their intangible assets and their financing set-up. The required information includes both external financing sources and internal financing policy.

In addition, many groups are also required to submit a yearly tax form which provides tax authorities with a global snapshot, per location, of revenues, taxes due and employees. For some treasury entities, this might trigger red flags and result in a visit from the tax inspector.

Safeguarding personal data

Technology and digital transformation play a crucial role for corporates in their quest for risk resilience and regulatory compliance. Large amounts of personal data are processed and used every day and, to safeguard it, the EU is imposing rigorous compliance rules under the General Data Protection Regulation (GDPR), which comes into effect in May 2018.

The GDPR drives corporates to ensure that the national privacy laws and procedures already in place match the new regulation. Carrying significant fines of up to €20 million or 4% of annual turnover – whichever is greater – and potential public disclosure in case of breach, this regulation obliges the full attention of Chief Information Security Officers (CISOs) and board members.

GDPR: should treasurers be concerned?

Treasurers will play a key role in ensuring compliance since they are responsible for the various business processes associated with collecting, processing and transmitting the personal data that will be protected under GDPR, including:

- **Bank account reconciliations:** Customer data such as names and bank details, used in bank account reconciliation processes;
- **Bank account management:** Personal data of employees with authorised signatory role for bank account management purposes;
- **Payment factories:** GDPR will apply to vendor information, such as bank account information stored in the payment process, belonging to individuals and contractors;
- **Payroll:** In-house and third-party vendor payroll processing, which includes salary, names, account details and national identity information.

Within these processes, treasury will need to consider GDPR data control and data processing requirements in areas such as TMS and payment factories. For example, employee and personal customer data must be secured, and any transaction data no longer required must be deleted or archived.

While many treasuries already have privacy protection in place for transactional data such as encrypted salary payment files, they need to work hand-in-hand with the company's responsible officer, usually the Data Protection Officer (DPO), to address process gaps relating to GDPR readiness.

In any case, effort will be significant and the costs substantial. GDPR compliance requires close attention and a tailored approach to avoid overspend and eliminate the risk of non-compliance, and treasurers should play an important role in this process.

Regulation for payment services

A number of regulatory initiatives aiming to facilitate global business should ease the life of treasurers, among which is the EU Payment Services Directive (PSD2), which comes into force in January 2018.

PSD2 is a regulatory response to the fast-moving and highly-demanding customer payment space which sees new players entering a sector which was for years dominated by traditional financial services. PSD2's goal is to standardise and stimulate new payment methods, protect customers, improve security and harmonise pricing.

PSD2 is expected to significantly disrupt the banks' traditional business models. For example, banks will be forced to provide access to some parts of their systems and data through a mandated, secure application programming interface, or API, which will allow third parties to make payments for account holders via a payment initiation service (PIS) and retrieve real-time bank statement information through an account information service (AIS).

What it means to corporate treasurers:

- **Greater innovation and more possibilities to support business**

Third-party providers are not just competitors, they are game changers who will challenge banks and bring diversification and innovation to the table. But the disruptors, Fintechs and others, can also benefit from teaming up with banks to leverage their brand, scale and trust equity. This should result in a better and broader product portfolio for corporates, at a lower cost.

From just a few recent payment innovations, such as direct account-based payments, instant and cross-border payments, and mobile banking, it is clear that PSD2 incorporates this new way of thinking within the payment landscape.

- **Increased competition**

The arrival of new entrants leads to greater competition in a market already characterised by relatively low prices compared to the operational risk taken, and will undeniably put more pressure on pricing. The openness of financial services and systems will also increase transparency with regard to charges and fees, which can put an additional layer of pressure on pricing.

- **Beware of cyber risks**

Opening systems up to multiple parties makes them much more vulnerable to hacking and cyber-attacks. Strong authentication measures and security standards will be key, but not sufficient in themselves. CISOs will have to be vigilant and look at their broader cybersecurity strategies when working with these new players and technologies.

PSD2 is most certainly an important piece of legislation which, in combination with new technologies, could revolutionise the payment landscape, and even banking as we know it. For corporates, this revolution could have many business and operational benefits. Treasurers should therefore consider the broader set of solutions offered by banks, Fintechs, blockchain and other technologies when determining or reviewing overall payment and collection strategies. But given the complexity of implementing PSD2 (think liabilities and misalignment of APIs, for instance), the full benefits for the corporate may take more time to become apparent than anticipated.

Building resiliency

The mission of most corporate treasury departments is to safeguard corporate assets and mitigate risks within an often global organisational structure and with budgets constantly under pressure. So, the key question is how can treasurers build efficient and resilient functionality that allows them to comply with regulations, deal with disruption, proactively address upcoming changes and (ideally) take advantage of strategic opportunities.

Resilience is an organisation's ability to recognise and react to changes in its environment, to survive and to evolve. It allows businesses to seize opportunities hidden within risk events. Redirecting the conversation from "risk" to "resilience" leads more successfully to the desired outcome — preparedness.

Companies and their treasury departments understand that fiscal, economic and financial market reform will continue to evolve. They don't know how big the impact will be, or exactly where it will hit, but regardless of precise location and severity, they need to be prepared and have flexible strategies.

For treasury, this means focusing on key building blocks:

Get involve in drafting the regulation:

- Enter the debate - the corporate voice is appreciated and needed to help shape financial regulation.

Develop knowledge and awareness:

- Train staff through direct sessions and webinars, making this a core component of their ongoing development and education;
- Reward your people for keeping up to date, sharing knowledge, insights and media updates within treasury and, depending on its implications, with other company stakeholders.

Ensure your governance structure supports a new approach to regulatory, macroeconomic and geopolitical risk:

- Establish a comprehensive inventory of risks;
- Draft plans to deal with potentially disruptive market events;
- Implement a robust compliance programme in collaboration with other corporate and business stakeholders;
- Consider appointing a compliance person in treasury who can centralise knowledge;
- Develop appropriate remediation, response and communication plans.

Leverage innovative technologies:

- Use flexible and scalable technology architecture to gather, structure and organise data - similar data sets may be applied to various regulations, but structured in a different way;
- Establish a single source of truth – drive synergies across data sets and integrate them with external sources of information, such as financial institutions and market data providers;
- Consider leveraging innovative (cloud-based) reporting solutions to increase visibility, flexibility and accuracy in reporting, where traditional ERP and TMS systems typically fall short;
- Develop advanced risk analytics including scenario planning;
- Consider specialised tools and systems regulatory technology (regtech) to facilitate regulatory compliance through data consistency, in-built workflows and governance, and improved analytics to make sense of data.

KEY POINTS TO REMEMBER

- **Geopolitical change and the associated risks have added an additional layer of complexity and uncertainty for treasurers to manage. Conversely, they represent an excellent opportunity for treasurers to continue to raise their profiles and drive real business value.**
- **Safeguarding personal data is now a priority for the EU, and with the prospect of GDPR coming into effect in 2018, corporates must ensure that current privacy laws and procedures are compliant with the new regulation.**
- **An important aspect of building a resilient organisation for treasurers is knowledge sharing and awareness creation. Networking within and outside the organisation is key, and should be actively promoted.**
- **Treasurers benefit from working hand-in-hand with tax experts and by putting an acute focus on substance and transparency.**

CASE STUDY

Why treasury and tax must work hand in hand: the case of company XYZ

The evolving tax landscape impacts the way multinational treasurers operate. One of the biggest game changers has been the OECD's base erosion and profit shifting (BEPS) plan. Through its various action plans, the OECD is aiming to bring taxation rights closer to the country "where value is created", and their key focus is on substance and transparency. How does this affect company XYZ?

Pre-BEPS situation

- Intercompany funding was granted by the Group treasury centre except for two loans issued by a group affiliate "XYZ" to two other subsidiaries. XYZ has limited substance with two fly-in directors.
- Upon issuance of these two long-term loans, no clear analysis was carried out to determine the arm's-length interest rate, and no documentation was prepared to support the applied rate.
- Additionally, all the funding provided by the treasury centre is structured as one month roll-over loans, so that both the treasury team and its subsidiaries have full flexibility. Part of this funding relates to major CAPEX investments.

Post-BEPS situation

- **As part of the BEPS requirements,** the Group needs to file a yearly tax form giving a snapshot of its worldwide activities. In this report XYZ popped-up as a red flag: it qualified as an intercompany financing entity with very significant interest income, no employees and fairly limited amount of taxes paid. To anticipate questions from the tax authorities worldwide, the group reassessed its funding set-up.
Although there were valid historical reasons for the set-up, a detailed analysis showed that the structure no longer met current substance requirements. Taking no action in this respect could result in a major withholding tax leakage and the bulk of XYZ's profits could become taxable in the treasury centre. To avoid such undesired consequences, XYZ reassigned the two loans to the treasury centre and XYZ was liquidated.
- **Upon reassignment of the two loans**, the historical interest rates were also reassessed. The risk profile of each subsidiary, as well as all the relevant terms & conditions of the loans were taken into account for this economic analysis. It appeared that the interest rates applied were defendable from a tax point of view. Moreover, the analysis showed that the loan was considered structured in a "commercial rational manner" taking into account all the relevant facts. The two loans could thus be kept in place.
The analysis was formalised and now forms part of the local files of the treasury centre and the two subsidiaries. In the meantime, the files have been shared with the tax authorities as part of the new compliance requirements.
- **Additionally, all the subsidiaries** must file the group's transfer pricing master file, providing information on the internal intragroup financing, as well as external financing arrangements.. In this case, the intercompany financing policy must be reassessed, as the short-term roll-over loans issued by the treasury centre did not always align with how a "commercially rational third party" would have behaved.
Part of the intercompany funding is now structured as long-term bullet or amortising loans with substantially higher interest rates. The remainder of the funding covers day-to-day cash requirements, and has been kept under the short-term flexible loans. However, a procedure has been put in place to regularly update the related intercompany interest rates to keep pace with the market interest rates.
- **Corporate treasury will have to cooperate with its tax counterparts** more closely than before, since a financing set-up is only sustainable for tax purposes if it is fully in line with operational reality. Harshening interest deductibility rules will also impact the cost of debt and thus how groups structure their funding.

Disclaimer: This case study aims to illustrate the challenges faced by treasurers. Any resemblance to an existing organisation would therefore be fortuitous.

AUGMENTED RISK IN A DIGITAL WORLD

CYBER-SECURITY

The old adage that "a chain is only as strong as its weakest link" gets new life in the world of cybersecurity. Anyone within an organisation can be targeted by scammers and fraudsters, and if the right security policies are not in place, the most humble employee can give the game away.

To keep company data and resources secure, staff training is crucial, but is that enough? On its own, the answer is no - this type of risk should be fully integrated within company cybersecurity strategy, which must be regularly updated.

Digital and mobile: the danger zone

The move toward a digital and mobile world has brought with it a number of invaluable tools boosting the speed, safety and effectiveness of treasury operations. But this doesn't just help simplify the life of treasurers. While digitalisation presents fresh opportunities, it also exposes treasurers to new dangers and concerns, and internal and external threats.

Cybersecurity is not just the responsibility of IT departments - treasurers should also be aware of the dangers lurking in cyberspace. Using social engineering, criminals can access with ease all kinds of information stored on the Internet (via Facebook, LinkedIn, online news, and others) and use it to carry out targeted attacks. Cybersecurity, and how to combat it, are therefore important issues to be addressed by today's treasurer.

Time is of the essence

According to Verizon's 2016 *Data Breach Investigation Report*, data can be successfully exfiltrated within minutes of a breach, so when it comes to data fraud, time is of the essence. Interestingly, PwC's *The Global State of Information Security® Survey 2017* notes that of the 15% of respondents who reported that there had been a serious breach in their company, one in three did not know for how long the company had been breached and 24% thought the breach had lasted a day.

The human element in cyber-security is both good and bad.

The top causes of cyber breach reported in the survey were human error, lack of staff awareness of security risks, failure to follow a defined process, and external attacks specifically targeting an organisation. The implication that human psychology, poor judgement and a propensity for mistakes are key in understanding the current breach landscape are confirmed by the survey's incident response answers: the most frequent breach vector was social engineering or phishing (55%), followed by malware (49%) and human error (45%).

Regardless of the implementation of security awareness training programmes, the direct link between human action and breaches is hard to ignore. This also means that organisations need to keep the human factor in mind when considering threats and their risk. Phishing, malware and social engineering can already be partially prevented by implementing appropriate security measures within the IT environment, and constantly updating them.

Breaches have a direct financial impact: 79% of the PwC survey participants reported that they suffered direct financial losses as a result of a breach. About a third of the responders did not know the value of lost assets, while for 11% it was under €1,000, up to €250,000 for a further 20%, and up to €1 million for another 20%, while 16% reported losses of more than a million. Despite the increase in direct financial loss caused by breaches, respondents still confirm that what makes breaches worse is the cost of investigation and finding a fix, followed by reputational damage.

The survey also found an increasing trend towards investing in cybersecurity within organisations. Just 5% of participants did not invest in cybersecurity. About a third of survey participants say they spent between €10,000 and €50,000 in the previous year, and nearly 5% spent more than €1 million on cybersecurity. About a third of respondents did not know how much effort was put into cybersecurity by their organisations.

Advanced skills wanted

When incidents do occur, just under half of respondents make use of third-party firms. Most do so to temporarily augment internal staff skillsets, but very few increase their teams' capacities or first-responder ability. This suggests that internal security teams frequently operate without the necessary advanced skills.

Much emphasis is placed on building threat intelligence, and there is also increased spending on security tooling. However, when it comes to identifying compromised devices, user notifications or complaints are the most relied-upon methods. This human intrusion detection system is followed by more traditional alerts from firewalls, intrusion prevention systems, intrusion detection systems, unified threat management devices and log analysis.

The human element in cybersecurity is both good and bad. While on one hand, humans can cause issues by replying to phishing emails or opening malware, on the other hand, they are needed to identify potential incidents.

Asset recovery

To prevent falling victim to a cyber incident, it is important to establish an asset recovery or cyber incident plan. This plan should not only contain details of whom to contact internally, but also externally, as soon as an incident is discovered. As time is crucial when an attack happens, it is important to immediately start to identify the financial and reputational loss due to the attack. Where financial loss is concerned, every second counts. Financial institution partners should be notified quickly so that losses can potentially be recuperated.

For banks, as time passes it becomes significantly harder to recover funds stolen during an attack. After only 24 hours, the chances of recuperation drop substantially, making it nearly impossible to trace and recover funds. With this in mind, it is very important to build and maintain a mutually trusting relationship with the financial institutions your organisation relies upon.

Roles and responsibilities need to be communicated to assure optimal procedures to secure transactions against all fraudulent activities, ranging from card theft and account takeovers to CEO fraud. This is to the benefit of both parties, and not only does it help speed up the process of recovering lost funds, it also helps the financial institution to identify potentially malicious activity immediately it happens, so that they can act before funds are stolen. Incorporating advanced fraud analytics within the daily operations of treasury can also be critical in such situations, especially in relation to processes like instant payments.

To help protect corporate reputation, it is important to continually evaluate the situation as it develops and make sure stakeholders are kept informed. Having funds stolen is bad enough, without the general public learning about it before key stakeholders have been informed.

Practice is everything

In general, most companies already have a well-prepared plan to help them react to cyber incidents. However, it seems that in many cases, those plans rarely survive their first brush with reality, too often leaving incident responders and crisis managers facing unforeseen circumstances. Effective and efficient crisis response requires the right combination of skills, knowledge and experience from a range of corporate functions, all working together. It should bring together a combination of legal, human resources, media and public relations, privacy counsel, treasury, finance, corporate security, audit and shareholder relations.

Simulated attacks mimic what would happen if hackers were to penetrate certain systems within an organisation or agency. If a system is breached, infections could, in theory, impact the entire organisation, and simulated attacks are useful to help uncover flaws in cyberattack protocols. A common issue is not making the appropriate real-time critical decisions to mitigate threats. Simulated attacks can also help identify flaws in IT security. Regular simulations are far more valuable than the plans based on them. They help generate "muscle memory" for incident response, making the process, environment and decision-making construct second nature to stakeholders who will be under pressure in a crisis, so that they can focus on resolving the issue at hand.

Effective and efficient crisis response requires the right combination of skills, knowledge and experience.

In one example, a simulated attack was staged in a small corporate environment, where all 50 employees were notified in advance that it would take place. During the simulation, 35 of the 50 employees duly handed over their passwords or gave unauthorised access to the system. This scenario could also be imagined in larger enterprises.

False attacks, true results

Simulated attacks in all types of enterprises help executives or higher management to assess their readiness to respond to a breach and practise striking the appropriate balance between taking action and ensuring that the necessary cybersecurity measures are available and properly used.

Through simulated attacks staged at team level, or in whole organisations, employees become more aware of their roles and responsibilities when real incidents occur. Demonstrating to the public, and stakeholders, that these kinds of exercises are carried out will also further cement trust in the organisation.

Know your predators

In a technology-driven world, threats lurk around every corner. It is almost impossible to predict an attack in advance, but knowing the work environment and keeping staff aware of cybersecurity trends are key factors when considering who are the adversaries. Criminals who choose to target your organisation will most likely attack your most valuable assets for personal financial gain.

Staff should be made aware of the potential value - both financial and reputational - of their work and the assets used to produce it. Company documents sold on the black market could have a considerably greater financial impact than simply loss of funds. An organisation's reputation and level of public trust could also be greatly affected by the leaking of documents.

It is not always feasible to ensure the security of all company assets. By determining your critical assets - your 'crown jewels' - it can be easier to protect them. Within treasury it is important to constantly update an inventory of threats, whether they involve or are directed at the cloud, e-banking, TMS, or payment software. By assessing the threat and the assets at risk you can establish a risk matrix for your assets.

It is a company-wide responsibility to keep up-to-date with current cyber security developments by means of online information and newsletters, to help the enterprise better protect assets against new potential vulnerabilities. This provides an overview of live threats in the landscape, but collaborating with global organisations to share information brings more insights into threats specific to treasury. Such threats are cross-border, so communicating with other companies could potentially save another organisation. As in any other sector, attackers evolve their skills and will, over time, find new ways to attack.

Bogus files and fake websites

No company can consider itself safe today. Many incidents occur because employees are unaware of the need to be vigilant, while attackers can easily, and in very cost-efficient ways, spam employees with files or links to websites containing malicious code, as famously happened in the Google Docs phishing attempt of May 2017.

Opening bogus files or visiting fake websites can immediately compromise a company, and its assets can be extracted from the company's infrastructure, leading to financial and reputational loss. The costs can include data damage and loss, downtime, lost productivity, forensic investigation, restoration and deletion of hostage data and systems, and reputational harm.

Employee training has been stepped up as a direct response to attacks using ransomware, a new model that monetises bitcoin breaches. Ransomware is a malicious software that can threaten to publish the victim's data or perpetually block access to it unless a ransom is paid. Forewarned is forearmed, but targeted attacks have grown in sophistication such that even preparation is insufficient, and to be forearmed requires a robust and practised incident response capability.

Footnote - A phishing attempt by an unknown hacker using Google Docs. Targets received an email stating that a user wanted to share a document with them. By clicking the fake link and logging into what they thought was their Google account, they put their details in the hands of the attacker. The virus was then spread to all the target's contacts. Google has taken action to prevent this kind of attack in the future.

KEY POINTS TO REMEMBER

- **Individual staff are increasingly targeted and continue to be an organisation's weakest link. Increased security awareness training, as currently practised, does not appear to be having much effect on the rate of breaches, and therefore this type of risk should be better integrated within company cybersecurity strategy, and regularly updated.**
- **Know your incident plan and make sure all internal stakeholders are aware of it. Have a plan to react, and test it regularly.**
- **Breaches do not just result in direct financial loss, but entail additional costs for investigation and resolution. There is also a risk of reputational damage where a breach is leaked to the public. Consider implementing bug-bounty programmes, or involve ethical hackers to locate potential security holes before attackers do. When breaches occur, be sure to communicate this in a timely manner to stakeholders and the public.**
- **As part of an overall approach to prevent and manage fraud, a leading agro-industrial group adapted its internal culture and updated agreements with its financial partner.**

CASE STUDY

Royal Cosun vs. social engineering fraud

Royal Cosun, an agro-industrial group that processes crops and other vegetable raw materials, became a victim of a social engineering scam which resulted in a fraudulent payment to a foreign bank account. The fraud was discovered during a forensic analysis of electronic data, from mailboxes, computers and smartphones, and interviews with employees.

The incident began with a spoof email providing context and instructions on how to deal with an ongoing confidential transaction, supposedly from a senior manager. Email correspondence continued after the original mail, involving a payment up to the maximum allowed amount to a foreign bank account. This was supported by incoming and outgoing telephone calls with a bogus French lawyer who was supposedly involved in the confidential transaction. Using flattery, threats and appeals to higher authority the lawyer emphasised the importance, urgency and secrecy of the transaction, and in less than 24 hours, the damage was done.

This use of electronic and real-person manipulation is an increasing threat, and has severe consequences requiring a pragmatic solution. While technology facilitates the transfers, the targets of the fraudsters' attacks are your colleagues. After the fact, some companies want to believe that it should be another party's responsibility to verify transactions. Some choose to buy cyber insurance as an "airbag" safety measure. However, the best protection is engagement with employees and a strong culture of openness, validation and support, making employees aware of the dangers.

After this incident of social engineering, Royal Cosun moved quickly to make two major changes: adapting the company's internal culture and updating agreements with its financial institution.

Preventing : do's and dont's

Learning from cases like Royal Cosun, here are some tips to avoid social engineering fraud:

- **Do not rely on verification and validation by a third party**
Always record all verifications made on payment instructions before making any payment. This may mean that a supplier has to wait an additional day or has to send a reminder, but the consequences of social engineering fraud are potentially much worse.

- **Communicate any event that seems out of the ordinary, and raise the alarm if you think you may have been targeted**
Make the bridge between employees and management as easy as possible. Employees should not be afraid to communicate fears to management or their security department.

- **Do not share certain types of information on social media**
Information from social media, such as Facebook status, vacation plans and photos, or very specific LinkedIn job titles, are used by the professional fraudster to research social engineering attacks. Criminals conduct research on the victim, so that the story appears plausible, and often social media is used for that purpose. For instance, if an out-of-office reply mentions that someone is not available for three weeks during summer, a social engineering fraudster will know this absence is not a business trip and will adapt the story to the circumstances.

- **Payment approval by phone or fax should not be trusted**
Only payments going through the normal approval system should be executed. Well-functioning call-back procedures should also be put in place.

Once the communication stream between management and employees has been established, and agreements are made with the financial institution, much better protection will be in place to combat this kind of fraudulent activity.

CLOSING THOUGHTS

Resilience, and a company's ability to survive and evolve to seize hidden opportunities, is also at the heart of these *Journeys to Treasury*.

Journeys to Treasury is an ongoing investigation, a series of selected trends and events impacting the world of corporate treasurers, today and into the future. It is a unique initiative, the fruit of co-creation between four leading players in corporate treasury: the bank; the association; the consultant; and the systems vendor.

In 2017, regulation and compliance have been uppermost in the minds of treasurers and corporates, and with good reason. It is tempting to lapse into a kind of panic over financial uncertainties, and indeed the accelerated momentum of a changing world, but looking beyond the headlines reveals that those with cool heads are finding ways to navigate the choppy waters successfully. Sitting back and reflecting upon what we see and feel, sharing with experts and with our peers, analysing and making smart assumptions, all are of the essence in order to make sense of a complex, transforming environment.

We have seen how smart corporates are leveraging innovative technologies to help in decision-making, and how involving staff at all levels, through training and information-sharing, can combat cyber-attacks, and inform the response to regulatory issues.

Resilience, and the ability for a company to survive and evolve to seize hidden opportunities is also at the heart of these Journeys to Treasury. Treasury is well-placed, but will need to consult and engage with other stakeholders within and outside the organisation to find the building blocks for agile responses to challenges.

If you would like to comment on any of the topics covered in this second edition of the publication, or would like to add your thoughts and ideas to the 2018 edition, visit www.journeystotreasury.com.

Disclaimer

BNP Paribas

About BNP Paribas Cash Management

BNP Paribas provides cash management services to more than 40,000 corporate clients around the world. Through its local presence on all continents, BNP Paribas is able to accompany corporates across the world. Our community of 2,500 experienced, committed Cash Management professionals operate across BNP Paribas' international network, in 208 business centres in 55 countries, covering more than 130 currencies. BNP Paribas has been designated No. 1 Trade Finance Bank and No. 1 Cash Management Bank in the European large corporate sector, in the latest Greenwich Associates research.

www.cashmanagement.bnpparibas.com

EACT

The European Association of Corporate Treasurers (EACT) is a grouping of national associations representing treasury and finance professionals in 20 countries in Europe, and brings together about 13,000 members representing 6,500 groups and companies. The association offers commentary to the European authorities, national governments, regulators and standard-setters on issues faced by treasury and finance professionals across Europe, and seeks to encourage the profession of treasury, corporate finance and risk management, promoting the value of treasury skills through best practice and education.

www.eact.eu

PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.be. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.

www.pwc.com/structure

SAP

As the market leader in enterprise application software, SAP is at the centre of today's business and technology transformation to a digital world. SAP has a comprehensive suite of solutions for treasury management driven by SAP S/4HANA in-memory technology. The combination of transactional data and business insights helps Treasurers gain greater insight and control over complex processes for managing payments, cash, liquidity, and risk, while integrating financial reporting and accounting within one single system.

By optimizing working capital, risk management, and compliance, treasury managers can gain complete transparency into and control over the entire portfolio and automate critical processes. With SAP, you can either deploy on premise or rely on proven enterprise cloud security and hosting services with 110 million cloud subscribers and 41 state-of-the-art data centers around the world – and choose from a public, private, or hybrid cloud environment. SAP innovations help 355,000 customers worldwide work together more efficiently and use business insight more effectively.

For more information, visit **www.sap.com/treasury**

Managing editors
Jean-François Denis, Deputy Head of Cash Management, BNP Paribas • **Christian Mnich**, Senior Director Treasury and Risk Management SAP • **Jean-Marc Servat**, Chairman of EACT (European Association of Corporate Treasurers) • **Didier Vandenhaute**, Partner Treasury Advisory, PwC

Contributors
BNP Paribas
Jan De Blauwe, Chief Information Security Officer • **Henri Eydoux**, Fraud prevention • **Wim Grosemans**, Head of International Payments • **Steven Lenaerts**, Head of Global Channels • **Bruno Mellado**, Head of Payments & Collections international • **Gautier Mouzelard**, Head of Compliance Projects • **Jan Dirk Van Beusekom**, Executive Director Cash Management • **Patrick Wheeler**, Consultant

EACT
Richard Cordero, Chief Operating Officer - EACT • **Guillermo de la Fuente**, Board member - EACT, Chairman - ACTSR • **Cornelia Hesse**, Board member - EACT, Board member - VDT, Head of controlling - BASF Services Europe GmbH • **Anni Mykkänen**, Policy Advisor - EACT • Delegates to the EACT Summit

SAP
Christian Mnich, Senior Director Treasury and Risk Management • **Uwe Erdtmann**, Solution Marketing • **Thomas Frenehard**, Director Solution Management, Governance, Risk and Compliance

PwC
Karla Bemelmans, Senior Manager Risk Assurance Solutions • **Hans Candries**, Partner Treasury Advisory • **Koen De Smet**, Senior Manager Treasury Advisory • **David Ledure**, Partner Corporate Tax Advisory • **Damien McMahon**, Partner Treasury Advisory • **Didier Vandenhaute**, Partner Treasury Advisory • **Marco van Harten**, Senior Manager Treasury Advisory

External experts
Jeroen Helders, Group Treasurer, Royal Cosun • **Antonio Nota**, Group Treasurer, Givaudan • **Anja Stranz**, Head of Cash Management, Vattenfall

THANK YOU

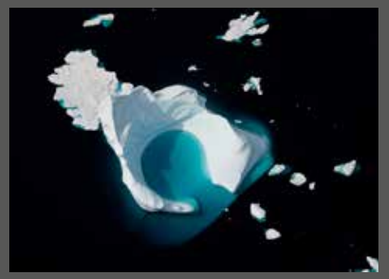
Photo credit
Getty Images

Project steering: Carole Djen-Ullmo, Head of Communication & Marketing, BNP Paribas Cash Management **& Hajar Diouri,** Consultant • **Copywriting: Bo Jones**, PwC, **Andrew Wilson** & **Katia Fau**


Montenegro


Netherlands


Netherlands


Greenland


Montenegro

JOIN US ON
WWW.JOURNEYSTOTREASURY.COM

BNP PARIBAS
The bank for a changing world

EACT THE EUROPEAN ASSOCIATION OF CORPORATE TREASURERS

pwc

SAP